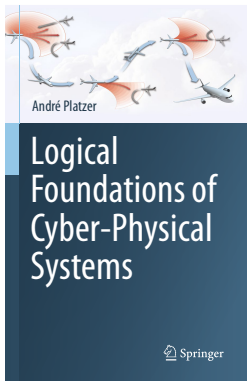


# 20: Virtual Substitution & Real Equations

## Logical Foundations of Cyber-Physical Systems



André Platzer

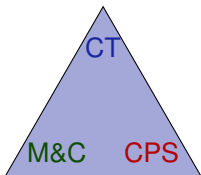
Karlsruhe Institute of Technology  
Department of Informatics

Computer Science Department  
Carnegie Mellon University

- 1 Learning Objectives
- 2 Framing the Miracle
- 3 Quantifier Elimination
  - Homomorphic Normalization for QE
  - Term Substitutions for Linear Equations
- 4 Square Root  $\sqrt{\cdot}$  Virtual Substitution for Quadratics
  - Square Root Algebra
  - Virtual Substitutions of Square Roots
  - Example
- 5 Summary

- 1 Learning Objectives
- 2 Framing the Miracle
- 3 Quantifier Elimination
  - Homomorphic Normalization for QE
  - Term Substitutions for Linear Equations
- 4 Square Root  $\sqrt{\cdot}$  Virtual Substitution for Quadratics
  - Square Root Algebra
  - Virtual Substitutions of Square Roots
  - Example
- 5 Summary

rigorous arithmetical reasoning  
miracle of quantifier elimination  
logical trinity for reals  
switch between syntax & semantics at will  
virtual substitution lemma  
bridge gap between semantics and inexpressibles



analytic complexity  
modeling tradeoffs

verifying CPS at scale

- 1 Learning Objectives
- 2 Framing the Miracle
- 3 Quantifier Elimination
  - Homomorphic Normalization for QE
  - Term Substitutions for Linear Equations
- 4 Square Root  $\sqrt{\cdot}$  Virtual Substitution for Quadratics
  - Square Root Algebra
  - Virtual Substitutions of Square Roots
  - Example
- 5 Summary

$$x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2$$

When  $\omega(x) = 2$

$$\omega[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2]$$

When  $\omega(x) = 2$

$$\omega[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2] = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \textit{false}$$



When  $\omega(x) = 2$

$$\omega[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2] = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \textit{false}$$

When  $v(x) = -1$

$$v[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2]$$

When  $\omega(x) = 2$

$$\omega[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2] = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \textit{false}$$

When  $v(x) = -1$

$$v[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2] = (-1)^2 > 2 \wedge 2 \cdot (-1) < 3 \vee (-1)^3 \leq (-1)^2 = \textit{true}$$

When  $\omega(x) = 2$

$$\omega \llbracket x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2 \rrbracket = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \text{false}$$

When  $\nu(x) = -1$

$$\nu \llbracket x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2 \rrbracket = (-1)^2 > 2 \wedge 2 \cdot (-1) < 3 \vee (-1)^3 \leq (-1)^2 = \text{true}$$

Are the following formulas valid, i.e., true in all states?

$$x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2$$

$$\forall x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

$$\exists x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

When  $\omega(x) = 2$

$$\omega[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2] = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \text{false}$$

When  $\nu(x) = -1$

$$\nu[x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2] = (-1)^2 > 2 \wedge 2 \cdot (-1) < 3 \vee (-1)^3 \leq (-1)^2 = \text{true}$$

Are the following formulas valid, i.e., true in all states?

$$\not\vdash x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2$$

$$\forall x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

$$\exists x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

When  $\omega(x) = 2$

$$\omega \llbracket x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2 \rrbracket = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \text{false}$$

When  $\nu(x) = -1$

$$\nu \llbracket x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2 \rrbracket = (-1)^2 > 2 \wedge 2 \cdot (-1) < 3 \vee (-1)^3 \leq (-1)^2 = \text{true}$$

Are the following formulas valid, i.e., true in all states?

$$\not\models x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2$$

$$\not\models \forall x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

$$\exists x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

When  $\omega(x) = 2$

$$\omega \llbracket x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2 \rrbracket = 2^2 > 2 \wedge 2 \cdot 2 < 3 \vee 2^3 \leq 2^2 = \text{false}$$

When  $\nu(x) = -1$

$$\nu \llbracket x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2 \rrbracket = (-1)^2 > 2 \wedge 2 \cdot (-1) < 3 \vee (-1)^3 \leq (-1)^2 = \text{true}$$

Are the following formulas valid, i.e., true in all states?

$$\not\models x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2$$

$$\not\models \forall x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

$$\models \exists x (x^2 > 2 \wedge 2x < 3 \vee x^3 \leq x^2)$$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- 1 Propositional logic [no variables]
- ✓ FOL[ $p, f, \dots$ ] uninterpreted
- 2 FOL $_{\mathbb{N}}$ [ $+, \cdot, =$ ]
- 3 FOL $_{\mathbb{R}}$ [ $+, \cdot, =, <$ ]
- 4 FOL $_{\mathbb{Q}}$ [ $+, \cdot, =$ ]
- 5 FOL $_{\mathbb{C}}$ [ $+, \cdot, =$ ]

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



✓ Propositional logic [no variables]

decidable

✓ FOL[ $p, f, \dots$ ] uninterpreted

2 FOL $_{\mathbb{N}}$ [ $+, \cdot, =$ ]

3 FOL $_{\mathbb{R}}$ [ $+, \cdot, =, <$ ]

4 FOL $_{\mathbb{Q}}$ [ $+, \cdot, =$ ]

5 FOL $_{\mathbb{C}}$ [ $+, \cdot, =$ ]



Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for: 

- ✓ Propositional logic [no variables] decidable
- ✓ FOL[ $p, f, \dots$ ] uninterpreted semidecidable [Gödel'30, Herbrand'30]
- 2 FOL $_{\mathbb{N}}$ [ $+, \cdot, =$ ]
- 3 FOL $_{\mathbb{R}}$ [ $+, \cdot, =, <$ ]
- 4 FOL $_{\mathbb{Q}}$ [ $+, \cdot, =$ ]
- 5 FOL $_{\mathbb{C}}$ [ $+, \cdot, =$ ]

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for: 

- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ③  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$
- ④  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$
- ⑤  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for: 

- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ④  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$
- ⑤  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for: 

- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$  not semidecidable [Robinson'49]
- 5  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for: 

- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$   $\sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}_{\mathbb{R}}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =] \sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]
- 6  $\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$
- 7  $\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$
- 8  $\text{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$
- 9  $\text{FOL}_{\mathbb{R}}[+, \cdot, \text{exp}, =, <]$
- 10  $\text{FOL}_{\mathbb{R}}[+, \cdot, \text{sin}, =, <]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}_{\mathbb{R}}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =] \sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]
- ✓  $\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$  decidable Gaussian elim. [179 CE]
- 7  $\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$
- 8  $\text{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$
- 9  $\text{FOL}_{\mathbb{R}}[+, \cdot, \text{exp}, =, <]$
- 10  $\text{FOL}_{\mathbb{R}}[+, \cdot, \text{sin}, =, <]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}_{\mathbb{P}}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$   $\sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]
- ✓  $\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$  decidable Gaussian elim. [179 CE]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$  decidable [Fourier 1826]
- 8  $\text{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$
- 9  $\text{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$
- 10  $\text{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$



Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}_{\mathbb{P}}[p, f, \dots]$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =] \sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]
- ✓  $\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$  decidable Gaussian elim. [179 CE]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$  decidable [Fourier 1826]
- ✓  $\text{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$  decidable [Presburger'29, Skolem'31]
- 9  $\text{FOL}_{\mathbb{R}}[+, \cdot, \exp, =, <]$
- 10  $\text{FOL}_{\mathbb{R}}[+, \cdot, \sin, =, <]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- ✓ Propositional logic [no variables] decidable
- ✓  $FOL_{[p, f, \dots]}$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $FOL_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $FOL_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $FOL_{\mathbb{Q}}[+, \cdot, =] \sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $FOL_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]
- ✓  $FOL_{\mathbb{R}}[+, =, \wedge, \exists]$  decidable Gaussian elim. [179 CE]
- ✓  $FOL_{\mathbb{R}}[+, \leq, \wedge, \exists]$  decidable [Fourier 1826]
- ✓  $FOL_{\mathbb{N}}[+, =, 2|, 3|, \dots]$  decidable [Presburger'29, Skolem'31]
- ?  $FOL_{\mathbb{R}}[+, \cdot, \exp, =, <]$  Tarski's problem
- 10  $FOL_{\mathbb{R}}[+, \cdot, \sin, =, <]$

Is validity of formulas

decidable/semidecidable/undecidable/not semidecidable for:



- ✓ Propositional logic [no variables] decidable
- ✓  $\text{FOL}_{[p, f, \dots]}$  uninterpreted semidecidable [Gödel'30, Herbrand'30]
- ×  $\text{FOL}_{\mathbb{N}}[+, \cdot, =]$  Peano arithmetic not semidecidable [Gödel'31]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \cdot, =, <]$  decidable [Tarski'31..51]
- ×  $\text{FOL}_{\mathbb{Q}}[+, \cdot, =]$   $\sqrt{2} \notin \mathbb{Q}, \exists x x^2 = 2$  not semidecidable [Robinson'49]
- ✓  $\text{FOL}_{\mathbb{C}}[+, \cdot, =]$  decidable [Tarski'51, Chevalley'51]
- ✓  $\text{FOL}_{\mathbb{R}}[+, =, \wedge, \exists]$  decidable Gaussian elim. [179 CE]
- ✓  $\text{FOL}_{\mathbb{R}}[+, \leq, \wedge, \exists]$  decidable [Fourier 1826]
- ✓  $\text{FOL}_{\mathbb{N}}[+, =, 2|, 3|, \dots]$  decidable [Presburger'29, Skolem'31]
- ?  $\text{FOL}_{\mathbb{R}}[+, \cdot, \text{exp}, =, <]$  Tarski's problem
- ×  $\text{FOL}_{\mathbb{R}}[+, \cdot, \text{sin}, =, <]$   $\text{sin } x = 0$  not semidecidable [Richardson'68]



1 Learning Objectives

2 Framing the Miracle

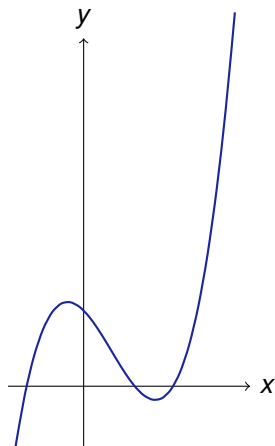
3 **Quantifier Elimination**

- Homomorphic Normalization for QE
- Term Substitutions for Linear Equations

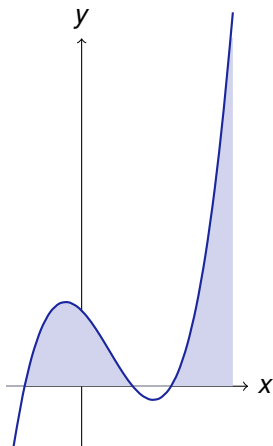
4 Square Root  $\sqrt{\cdot}$  Virtual Substitution for Quadratics

- Square Root Algebra
- Virtual Substitutions of Square Roots
- Example

5 Summary

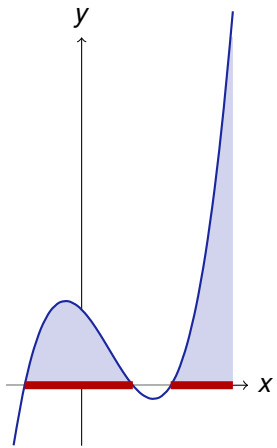


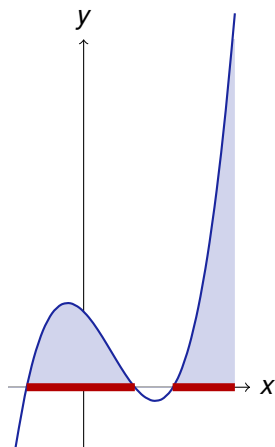
$$F \equiv \exists y (y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$



$$F \equiv \exists y (y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$

$$F \equiv \exists y (y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$





$$F \equiv \exists y (y \geq 0 \wedge 1 - x - 1.83x^2 + 1.66x^3 > y)$$



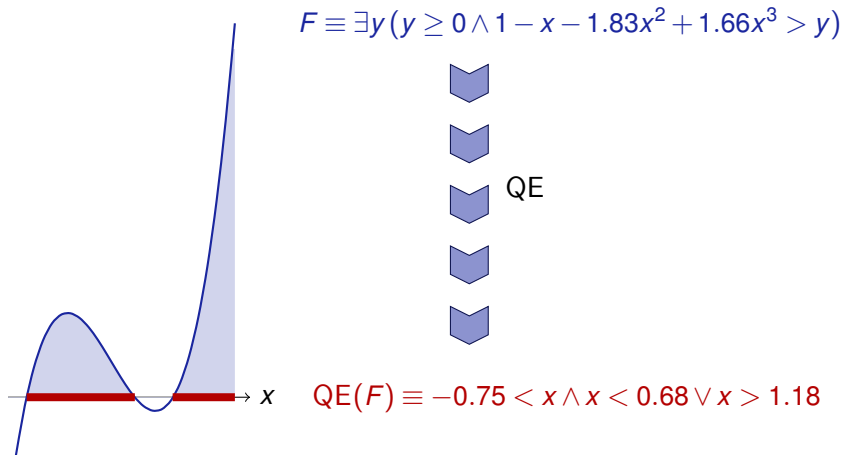
$$QE(F) \equiv -0.75 < x \wedge x < 0.68 \vee x > 1.18$$



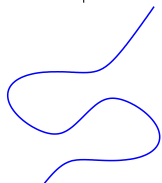
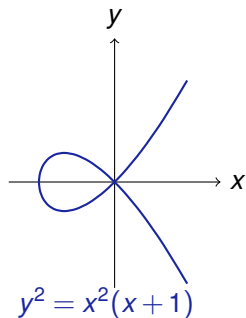
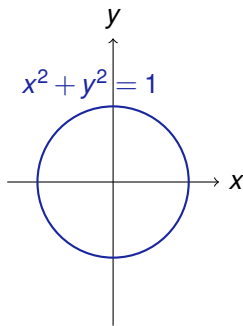
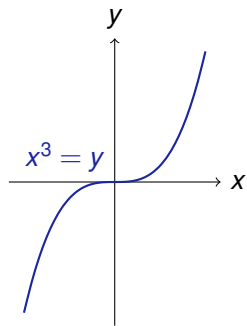


A horizontal number line with an arrow pointing to the right, labeled with the variable  $x$ . Two thick red horizontal bars are drawn above the line, representing intervals. The first bar starts at a point and ends at another point. The second bar starts at a point further to the right and ends at a point further to the right. The two bars do not overlap.

$$\text{QE}(F) \equiv -0.75 < x \wedge x < 0.68 \vee x > 1.18$$

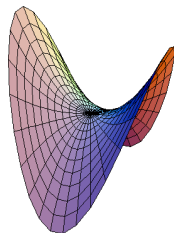


If all but one variable has fixed value: Finite union of intervals.  
 Univariate polynomials have finitely many roots. Signs change finitely often.

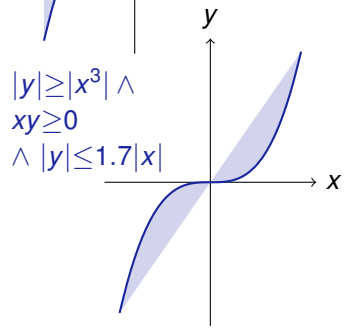
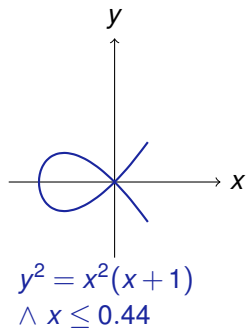
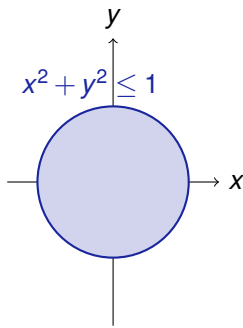
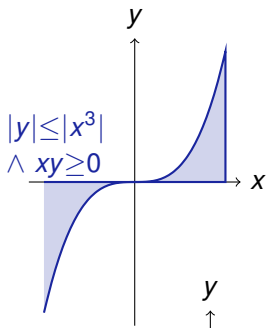


$$4x^3 + 4x^2y + 9xy^2 - 9y^3 - 36x + 36y = 0$$

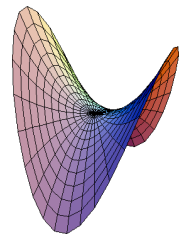
$$z = x^2 - y^2$$



Algebraic variety: defined by conjunction of polynomial equations



$z = x^2 - y^2$



## Theorem (Tarski'31)

*First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e., for each formula  $P$ , compute quantifier-free formula  $QE(P)$  that is equivalent, i.e.,  $P \leftrightarrow QE(P)$  is valid.*

## Theorem (Tarski'31)

*First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e., for each formula  $P$ , compute quantifier-free formula  $QE(P)$  that is equivalent, i.e.,  $P \leftrightarrow QE(P)$  is valid.*

## Theorem (Complexity, Davenport&Heintz'88, Weispfenning'88)

*(Time and space) complexity of QE for  $\mathbb{R}$  is doubly exponential in the number  $n$  of quantifier (alternations).*

$$2^{2^{O(n)}}$$

## Theorem (Tarski'31)

*First-order logic of real arithmetic is decidable since it admits quantifier elimination, i.e., for each formula  $P$ , compute quantifier-free formula  $QE(P)$  that is equivalent, i.e.,  $P \leftrightarrow QE(P)$  is valid.*

## Theorem (Complexity, Davenport&Heintz'88, Weispfenning'88)

*(Time and space) complexity of QE for  $\mathbb{R}$  is doubly exponential in the number  $n$  of quantifier (alternations).*

$$2^{2^{O(n)}}$$

Answer even for one *free* variable and only linear polynomials

$$\text{QE}(\exists x(2x^2 + c \leq 5)) \equiv$$

$$\text{QE}(\forall c \exists x(2x^2 + c \leq 5)) \equiv$$

$$\text{QE}(\exists x(a = b + x^2)) \equiv$$

$$\text{QE}(\exists x(x^2 = 2)) \equiv$$

$$\text{QE}(\exists x(x^2 = 2 \wedge y = x)) \equiv$$



$$\text{QE}(\exists x(2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\text{QE}(\forall c \exists x(2x^2 + c \leq 5)) \equiv$$

$$\text{QE}(\exists x(a = b + x^2)) \equiv$$

$$\text{QE}(\exists x(x^2 = 2)) \equiv$$

$$\text{QE}(\exists x(x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\text{QE}(\forall c \exists x (2x^2 + c \leq 5)) \equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5)))$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\text{QE}(\forall c \exists x (2x^2 + c \leq 5)) \equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5))$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\begin{aligned} \text{QE}(\forall c \exists x (2x^2 + c \leq 5)) &\equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5)) \\ &\equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \end{aligned}$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\begin{aligned} \text{QE}(\forall c \exists x (2x^2 + c \leq 5)) &\equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5)) \\ &\equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \textit{false} \end{aligned}$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\begin{aligned} \text{QE}(\forall c \exists x (2x^2 + c \leq 5)) &\equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5)) \\ &\equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \textit{false} \end{aligned}$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv a \geq b$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\begin{aligned} \text{QE}(\forall c \exists x (2x^2 + c \leq 5)) &\equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5)) \\ &\equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \textit{false} \end{aligned}$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv a \geq b$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv \textit{true}$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv$$

$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\begin{aligned} \text{QE}(\forall c \exists x (2x^2 + c \leq 5)) &\equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5)) \\ &\equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \textit{false} \end{aligned}$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv a \geq b$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv \textit{true}$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv y = \pm\sqrt{2}$$



$$\text{QE}(\exists x (2x^2 + c \leq 5)) \equiv c \leq 5$$

$$\begin{aligned} \text{QE}(\forall c \exists x (2x^2 + c \leq 5)) &\equiv \text{QE}(\forall c \text{QE}(\exists x (2x^2 + c \leq 5))) \equiv \text{QE}(\forall c (c \leq 5)) \\ &\equiv -100 \leq 5 \wedge 5 \leq 5 \wedge 100 \leq 5 \equiv \textit{false} \end{aligned}$$

$$\text{QE}(\exists x (a = b + x^2)) \equiv a \geq b$$

$$\text{QE}(\exists x (x^2 = 2)) \equiv \textit{true}$$

$$\text{QE}(\exists x (x^2 = 2 \wedge y = x)) \equiv y = \pm\sqrt{2} \equiv y^2 = 2$$

$$\text{QE}(A \wedge B) \equiv$$

$$\text{QE}(A \vee B) \equiv$$

$$\text{QE}(\neg A) \equiv$$

$$\text{QE}(\forall x A) \equiv$$

$$\text{QE}(\exists x A) \equiv$$

$A$  has quantifiers

$$\text{QE}(A \wedge B) \equiv \text{QE}(A) \wedge \text{QE}(B)$$

$$\text{QE}(A \vee B) \equiv \text{QE}(A) \vee \text{QE}(B)$$

$$\text{QE}(\neg A) \equiv \neg \text{QE}(A)$$

$$\text{QE}(\forall x A) \equiv \text{QE}(\neg \exists x \neg A)$$

$$\text{QE}(\exists x A) \equiv \text{QE}(\exists x \text{QE}(A))$$

$A$  has quantifiers

$$QE(A \wedge B) \equiv QE(A) \wedge QE(B)$$

$$QE(A \vee B) \equiv QE(A) \vee QE(B)$$

$$QE(\neg A) \equiv \neg QE(A)$$

$$QE(\forall x A) \equiv QE(\neg \exists x \neg A)$$

$$QE(\exists x A) \equiv QE(\exists x QE(A))$$

$A$  has quantifiers

$$QE(\exists x (A \vee B)) \equiv$$

$$QE(\exists x \neg (A \wedge B)) \equiv$$

$$QE(\exists x \neg (A \vee B)) \equiv$$

$$QE(\exists x \neg \neg A) \equiv$$

$$\text{QE}(A \wedge B) \equiv \text{QE}(A) \wedge \text{QE}(B)$$

$$\text{QE}(A \vee B) \equiv \text{QE}(A) \vee \text{QE}(B)$$

$$\text{QE}(\neg A) \equiv \neg \text{QE}(A)$$

$$\text{QE}(\forall x A) \equiv \text{QE}(\neg \exists x \neg A)$$

$$\text{QE}(\exists x A) \equiv \text{QE}(\exists x \text{QE}(A))$$

A has quantifiers

$$\text{QE}(\exists x (A \vee B)) \equiv \text{QE}(\exists x A) \vee \text{QE}(\exists x B)$$

$$\text{QE}(\exists x \neg (A \wedge B)) \equiv \text{QE}(\exists x (\neg A \vee \neg B))$$

$$\text{QE}(\exists x \neg (A \vee B)) \equiv \text{QE}(\exists x (\neg A \wedge \neg B))$$

$$\text{QE}(\exists x \neg \neg A) \equiv \text{QE}(\exists x A)$$



$$\text{QE}(A \wedge B) \equiv \text{QE}(A) \wedge \text{QE}(B)$$

$$\text{QE}(A \vee B) \equiv \text{QE}(A) \vee \text{QE}(B)$$

$$\text{QE}(\neg A) \equiv \neg \text{QE}(A)$$

$$\text{QE}(\forall x A) \equiv \text{QE}(\neg \exists x \neg A)$$

$$\text{QE}(\exists x A) \equiv \text{QE}(\exists x \text{QE}(A))$$

A has quantifiers

$$\text{QE}(\exists x (A \vee B)) \equiv \text{QE}(\exists x A) \vee \text{QE}(\exists x B)$$

$$\text{QE}(\exists x \neg (A \wedge B)) \equiv \text{QE}(\exists x (\neg A \vee \neg B))$$

$$\text{QE}(\exists x \neg (A \vee B)) \equiv \text{QE}(\exists x (\neg A \wedge \neg B))$$

$$\text{QE}(\exists x \neg \neg A) \equiv \text{QE}(\exists x A)$$

$$\text{QE}(\exists x (A \wedge (B \vee C))) \equiv$$

$$\text{QE}(\exists x ((A \vee B) \wedge C)) \equiv$$

$$\text{QE}(A \wedge B) \equiv \text{QE}(A) \wedge \text{QE}(B)$$

$$\text{QE}(A \vee B) \equiv \text{QE}(A) \vee \text{QE}(B)$$

$$\text{QE}(\neg A) \equiv \neg \text{QE}(A)$$

$$\text{QE}(\forall x A) \equiv \text{QE}(\neg \exists x \neg A)$$

$$\text{QE}(\exists x A) \equiv \text{QE}(\exists x \text{QE}(A))$$

A has quantifiers

$$\text{QE}(\exists x (A \vee B)) \equiv \text{QE}(\exists x A) \vee \text{QE}(\exists x B)$$

$$\text{QE}(\exists x \neg (A \wedge B)) \equiv \text{QE}(\exists x (\neg A \vee \neg B))$$

$$\text{QE}(\exists x \neg (A \vee B)) \equiv \text{QE}(\exists x (\neg A \wedge \neg B))$$

$$\text{QE}(\exists x \neg \neg A) \equiv \text{QE}(\exists x A)$$

$$\text{QE}(\exists x (A \wedge (B \vee C))) \equiv \text{QE}(\exists x ((A \wedge B) \vee (A \wedge C))) \quad \text{expensive}$$

$$\text{QE}(\exists x ((A \vee B) \wedge C)) \equiv \text{QE}(\exists x ((A \wedge C) \vee (B \wedge C))) \quad \text{expensive}$$

Normal Form  $QE(\exists x (A_1 \wedge \dots \wedge A_k))$  with atomic  $A_i$

$$QE(A \wedge B) \equiv QE(A) \wedge QE(B)$$

$$QE(A \vee B) \equiv QE(A) \vee QE(B)$$

$$QE(\neg A) \equiv \neg QE(A)$$

$$QE(\forall x A) \equiv QE(\neg \exists x \neg A)$$

$$QE(\exists x A) \equiv QE(\exists x QE(A))$$

$A$  has quantifiers

$$QE(\exists x (A \vee B)) \equiv QE(\exists x A) \vee QE(\exists x B)$$

$$QE(\exists x \neg (A \wedge B)) \equiv QE(\exists x (\neg A \vee \neg B))$$

$$QE(\exists x \neg (A \vee B)) \equiv QE(\exists x (\neg A \wedge \neg B))$$

$$QE(\exists x \neg \neg A) \equiv QE(\exists x A)$$

$$QE(\exists x (A \wedge (B \vee C))) \equiv QE(\exists x ((A \wedge B) \vee (A \wedge C))) \quad \text{expensive}$$

$$QE(\exists x ((A \vee B) \wedge C)) \equiv QE(\exists x ((A \wedge C) \vee (B \wedge C))) \quad \text{expensive}$$



Normal Form

 $QE(\exists x (p_1 \sim_i 0 \wedge \dots \wedge p_k \sim_k 0))$  and  $\sim_i \in \{>, =, \geq, \neq\}$ 

$$p = q \equiv p - q = 0$$

$$p \geq q \equiv p - q \geq 0$$

$$p > q \equiv p - q > 0$$

$$p \neq q \equiv p - q \neq 0$$

$$p \leq q \equiv q - p \geq 0$$

$$p < q \equiv q - p > 0$$

$$\neg(p \geq q) \equiv p < q$$

$$\neg(p > q) \equiv p \leq q$$

$$\neg(p = q) \equiv p \neq q$$

$$\neg(p \neq q) \equiv p = q$$

## Virtual Substitution

$$\exists x F \leftrightarrow \bigvee_{t \in T} A_t \wedge F_x^t$$

where terms  $T$  substituted (virtually) into  $F$  depend on  $F$   
where  $A_t$  are quantifier-free additional compatibility conditions

Scalability requires simplifier for intermediate results

## Virtual Substitution

$$\text{Quantifier} \rightarrow \exists x F \leftrightarrow \bigvee_{t \in T} A_t \wedge F_x^t \leftarrow \text{Quantifier-free}$$

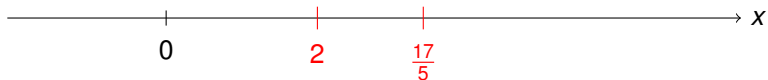
where terms  $T$  substituted (virtually) into  $F$  depend on  $F$   
where  $A_t$  are quantifier-free additional compatibility conditions

Scalability requires simplifier for intermediate results



Can we get rid of the quantifier without changing the semantics?

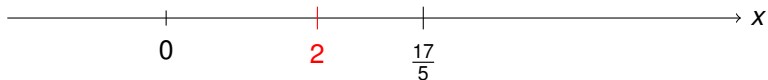
$$\exists x(x > 2 \wedge x < \frac{17}{5})$$



Can we get rid of the quantifier without changing the semantics?

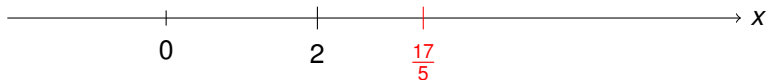
$$\exists x(x > 2 \wedge x < \frac{17}{5})$$

# Naïve Virtual Substitution by Example



Can we get rid of the quantifier without changing the semantics?

$$\begin{aligned} & \exists x(x > 2 \wedge x < \frac{17}{5}) \\ \equiv & (2 > 2 \wedge 2 < \frac{17}{5}) \qquad \text{boundary case "x = 2"} \end{aligned}$$

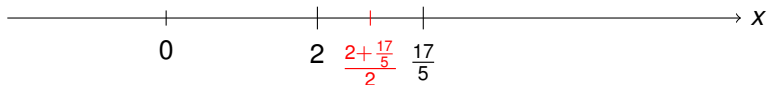


Can we get rid of the quantifier without changing the semantics?

$$\begin{aligned} & \exists x(x > 2 \wedge x < \frac{17}{5}) \\ \equiv & (2 > 2 \wedge 2 < \frac{17}{5}) \\ \vee & (\frac{17}{5} > 2 \wedge \frac{17}{5} < \frac{17}{5}) \end{aligned}$$

boundary case “ $x = 2$ ”

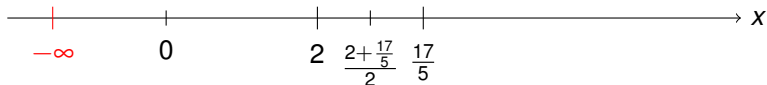
boundary case “ $x = \frac{17}{5}$ ”



Can we get rid of the quantifier without changing the semantics?

$$\begin{array}{ll}
 \exists x(x > 2 \wedge x < \frac{17}{5}) & \\
 \equiv (2 > 2 \wedge 2 < \frac{17}{5}) & \text{boundary case "x = 2"} \\
 \vee (\frac{17}{5} > 2 \wedge \frac{17}{5} < \frac{17}{5}) & \text{boundary case "x = } \frac{17}{5}\text{"} \\
 \vee (\frac{2 + \frac{17}{5}}{2} > 2 \wedge \frac{2 + \frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case "x = } \frac{2 + \frac{17}{5}}{2}\text{"}
 \end{array}$$

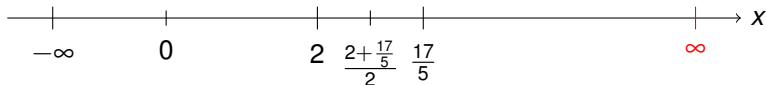




Can we get rid of the quantifier without changing the semantics?

$$\begin{array}{ll}
 \exists x(x > 2 \wedge x < \frac{17}{5}) & \\
 \equiv (2 > 2 \wedge 2 < \frac{17}{5}) & \text{boundary case "x = 2"} \\
 \vee (\frac{17}{5} > 2 \wedge \frac{17}{5} < \frac{17}{5}) & \text{boundary case "x = } \frac{17}{5}\text{"} \\
 \vee (\frac{2+\frac{17}{5}}{2} > 2 \wedge \frac{2+\frac{17}{5}}{2} < \frac{17}{5}) & \text{intermediate case "x = } \frac{2+\frac{17}{5}}{2}\text{"} \\
 \vee (-\infty > 2 \wedge -\infty < \frac{17}{5}) & \text{extremal case "x = } -\infty\text{"}
 \end{array}$$

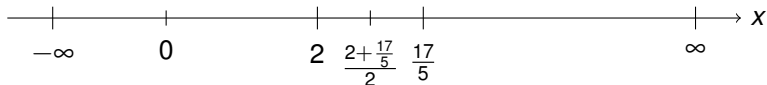
# Naïve Virtual Substitution by Example



Can we get rid of the quantifier without changing the semantics?

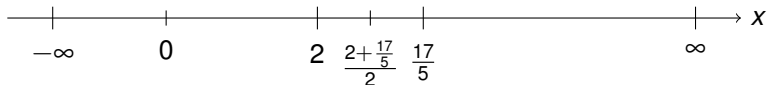
$\exists x(x > 2 \wedge x < \frac{17}{5})$	
$\equiv (2 > 2 \wedge 2 < \frac{17}{5})$	boundary case “ $x = 2$ ”
$\vee (\frac{17}{5} > 2 \wedge \frac{17}{5} < \frac{17}{5})$	boundary case “ $x = \frac{17}{5}$ ”
$\vee (\frac{2+\frac{17}{5}}{2} > 2 \wedge \frac{2+\frac{17}{5}}{2} < \frac{17}{5})$	intermediate case “ $x = \frac{2+\frac{17}{5}}{2}$ ”
$\vee (-\infty > 2 \wedge -\infty < \frac{17}{5})$	extremal case “ $x = -\infty$ ”
$\vee (\infty > 2 \wedge \infty < \frac{17}{5})$	extremal case “ $x = \infty$ ”

# Naïve Virtual Substitution by Example



Can we get rid of the quantifier without changing the semantics?

$\exists x(x > 2 \wedge x < \frac{17}{5})$	
$\equiv (2 > 2 \wedge 2 < \frac{17}{5})$	boundary case “ $x = 2$ ”
$\vee (\frac{17}{5} > 2 \wedge \frac{17}{5} < \frac{17}{5})$	boundary case “ $x = \frac{17}{5}$ ”
$\vee (\frac{2+\frac{17}{5}}{2} > 2 \wedge \frac{2+\frac{17}{5}}{2} < \frac{17}{5})$	intermediate case “ $x = \frac{2+\frac{17}{5}}{2}$ ”
$\vee (-\infty > 2 \wedge -\infty < \frac{17}{5})$	extremal case “ $x = -\infty$ ”
$\vee (\infty > 2 \wedge \infty < \frac{17}{5})$	extremal case “ $x = \infty$ ”
$\equiv \text{true}$	evaluate



Can we get rid of the quantifier without changing the semantics?

$\exists x(x > 2 \wedge x < \frac{17}{5})$	
$\equiv (2 > 2 \wedge 2 < \frac{17}{5})$	boundary case “ $x = 2$ ”
$\vee (\frac{17}{5} > 2 \wedge \frac{17}{5} < \frac{17}{5})$	boundary case “ $x = \frac{17}{5}$ ”
$\vee (\frac{2 + \frac{17}{5}}{2} > 2 \wedge \frac{2 + \frac{17}{5}}{2} < \frac{17}{5})$	intermediate case “ $x = \frac{2 + \frac{17}{5}}{2}$ ”
$\vee (-\infty > 2 \wedge -\infty < \frac{17}{5})$	extremal case “ $x = -\infty$ ”
$\vee (\infty > 2 \wedge \infty < \frac{17}{5})$	extremal case “ $x = \infty$ ”
$\equiv \textit{true}$	evaluate

- $\infty$  is not in  $\text{FOL}_{\mathbb{R}}$
- Interior points aren't always terms in  $\text{FOL}_{\mathbb{R}}$  if nonlinear
- Substituting them into formulas requires attention

## Theorem (Virtual Substitution: Linear Equation)

$$\exists x (bx + c = 0 \wedge F) \leftrightarrow$$

## Theorem (Virtual Substitution: Linear Equation)

$$\exists x (bx + c = 0 \wedge F) \leftrightarrow F_x^{-c/b}$$

Linear solution

## Theorem (Virtual Substitution: Linear Equation)

$$\exists x (bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b}$$

Don't divide by 0

## Theorem (Virtual Substitution: Linear Equation)

$$b \neq 0 \rightarrow (\exists x (bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b} )$$

Only actually linear solution if  $b \neq 0$



Theorem (Virtual Substitution: Linear Equation  $x \notin b, c$ )

$$b \neq 0 \rightarrow (\exists x (bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b}) \quad \text{if } x \notin b, c$$

Only linear if no  $x$  in  $b, c$

Theorem (Virtual Substitution: Linear Equation  $x \notin b, c$ )

$$b \neq 0 \rightarrow (\exists x (bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b}) \quad \text{if } x \notin b, c$$

Conditional equivalence, so conditions may need to be checked or case-split

Theorem (Virtual Substitution: Linear Equation  $x \notin b, c$ )

$$b \neq 0 \rightarrow (\exists x (bx + c = 0 \wedge F) \leftrightarrow b \neq 0 \wedge F_x^{-c/b}) \quad \text{if } x \notin b, c$$

Lemma (Uniform substitution of linear equations)

*The linear equation axiom is sound ( $b, c$  are arity 0 function symbols):*

$$\exists \text{lin } b \neq 0 \rightarrow (\exists x (b \cdot x + c = 0 \wedge q(x)) \leftrightarrow q(-c/b))$$

$$\exists x ((\underbrace{y^2 + 4}_b) \cdot x + (\underbrace{yz - 1}_c) = 0 \wedge x^3 + x \geq 0) \leftrightarrow \left(-\frac{yz - 1}{y^2 + 4}\right)^3 + \left(-\frac{yz - 1}{y^2 + 4}\right) \geq 0$$



- 1 Learning Objectives
- 2 Framing the Miracle
- 3 Quantifier Elimination
  - Homomorphic Normalization for QE
  - Term Substitutions for Linear Equations
- 4 Square Root  $\sqrt{\cdot}$  Virtual Substitution for Quadratics**
  - Square Root Algebra
  - Virtual Substitutions of Square Roots
  - Example
- 5 Summary

## Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

## Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$F_x^{(-b + \sqrt{b^2 - 4ac}) / (2a)}$$

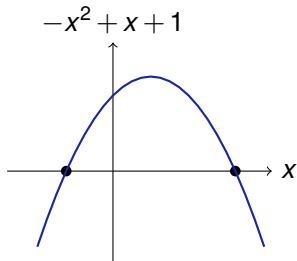
Quadratic solution

## Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$\left( F_x^{(-b + \sqrt{b^2 - 4ac}) / (2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac}) / (2a)} \right)$$

Or negative square root solution



## Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$a \neq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac}) / (2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac}) / (2a)} \right)$$

Don't divide by 0

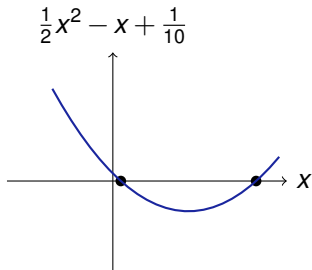


## Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge (F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)})$$

Real solution if  $\sqrt{\cdot}$  exists by discriminant



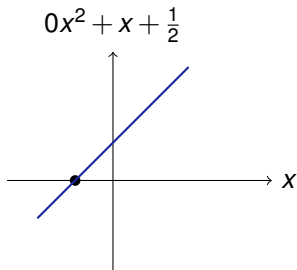
## Theorem (Virtual Substitution: Quadratic Equation)

$$\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge (F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)})$$

Instead linear solution if  $a = 0$  (may case-split)



## Theorem (Virtual Substitution: Quadratic Equation)

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

Only equivalent if not all 0 which gives trivial equation (else use  $F$ )

Theorem (Virtual Substitution: Quadratic Equation  $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

Only linear or quadratic if no  $x$  in  $a, b, c$

Theorem (Virtual Substitution: Quadratic Equation  $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent
- 2 Just not a formula ...

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent
- 2 Just not a formula ...
- 3  $(-b + \sqrt{b^2 - 4ac})/(2a)$  is not in  $\text{FOL}_{\mathbb{R}}$  and neither is  $-c/b$

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_x^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_x^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_x^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent
- 2 Just not a formula ...
- 3  $(-b + \sqrt{b^2 - 4ac})/(2a)$  is not in  $\text{FOL}_{\mathbb{R}}$  and neither is  $-c/b$
- 4 Virtual substitution  $F_{\bar{x}}^{(a+b\sqrt{c})/d}$  acts as if it were to substitute  $(a + b\sqrt{c})/d$  for  $x$  in  $F$



## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent
- 2 Just not a formula ...
- 3  $(-b + \sqrt{b^2 - 4ac})/(2a)$  is not in  $\text{FOL}_{\mathbb{R}}$  and neither is  $-c/b$
- 4 Virtual substitution  $F_{\bar{x}}^{(a+b\sqrt{c})/d}$  acts as if it were to substitute  $(a + b\sqrt{c})/d$  for  $x$  in  $F$  ... but it's merely equivalent

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent
- 2 Just not a formula ...
- 3  $(-b + \sqrt{b^2 - 4ac})/(2a)$  is not in  $\text{FOL}_{\mathbb{R}}$  and neither is  $-c/b$
- 4 Virtual substitution  $F_{\bar{x}}^{(a+b\sqrt{c})/d}$  acts as if it were to substitute  $(a + b\sqrt{c})/d$  for  $x$  in  $F$  ... but it's merely equivalent
- 5  $\exists r (r^2 = c)$  would do it for  $\sqrt{c}$

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

- 1 Quantifier-free equivalent
- 2 Just not a formula ...
- 3  $(-b + \sqrt{b^2 - 4ac})/(2a)$  is not in  $\text{FOL}_{\mathbb{R}}$  and neither is  $-c/b$
- 4 Virtual substitution  $F_{\bar{x}}^{(a+b\sqrt{c})/d}$  acts as if it were to substitute  $(a + b\sqrt{c})/d$  for  $x$  in  $F$  ... but it's merely equivalent
- 5  $\exists r (r^2 = c)$  would do it for  $\sqrt{c}$  but that's going in circles

Theorem (Virtual Substitution: Quadratic Equation  $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} \underline{\underline{\quad}}$$

Convention: On this slide  $c'$  is not a derivative but just another name . . .

## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a + b\sqrt{c})/d)$$

Convention: On this slide  $c'$  is not a derivative but just another name ...

## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\bar{x}}^{(a+b\sqrt{c})/d} \stackrel{\text{def}}{=} p((a + b\sqrt{c})/d) \quad \text{by algebraic evaluation of } +, \cdot$$

Convention: On this slide  $c'$  is not a derivative but just another name ...

## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\frac{a+b\sqrt{c}}{d}} \stackrel{\text{def}}{=} p\left(\frac{a+b\sqrt{c}}{d}\right) \quad \text{by algebraic evaluation of } +, \cdot$$

## $\sqrt{c}$ -algebra

Algebra of terms  $(a + b\sqrt{c})/d$  with polynomials  $a, b, c, d \in \mathbb{Q}[x_1, \dots, x_n]$ :

$$\left(\frac{a + b\sqrt{c}}{d}\right) + \left(\frac{a' + b'\sqrt{c}}{d'}\right) =$$

$$\left(\frac{a + b\sqrt{c}}{d}\right) \cdot \left(\frac{a' + b'\sqrt{c}}{d'}\right) =$$

Convention: On this slide  $c'$  is not a derivative but just another name ...



## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\frac{a+b\sqrt{c}}{d}} \stackrel{\text{def}}{=} p\left(\frac{a+b\sqrt{c}}{d}\right) \quad \text{by algebraic evaluation of } +, \cdot$$

## $\sqrt{c}$ -algebra

Algebra of terms  $(a + b\sqrt{c})/d$  with polynomials  $a, b, c, d \in \mathbb{Q}[x_1, \dots, x_n]$ :

$$\begin{aligned} ((a + b\sqrt{c})/d) + ((a' + b'\sqrt{c})/d') &= ((ad' + da') + (bd' + db')\sqrt{c})/(dd') \\ ((a + b\sqrt{c})/d) \cdot ((a' + b'\sqrt{c})/d') &= \end{aligned}$$

Convention: On this slide  $c'$  is not a derivative but just another name ...

## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\frac{a+b\sqrt{c}}{d}} \stackrel{\text{def}}{=} p\left(\frac{a+b\sqrt{c}}{d}\right) \quad \text{by algebraic evaluation of } +, \cdot$$

## $\sqrt{c}$ -algebra

Algebra of terms  $(a + b\sqrt{c})/d$  with polynomials  $a, b, c, d \in \mathbb{Q}[x_1, \dots, x_n]$ :

$$\begin{aligned} ((a + b\sqrt{c})/d) + ((a' + b'\sqrt{c})/d') &= ((ad' + da') + (bd' + db')\sqrt{c})/(dd') \\ ((a + b\sqrt{c})/d) \cdot ((a' + b'\sqrt{c})/d') &= ((aa' + bb'c) + (ab' + ba')\sqrt{c})/(dd') \end{aligned}$$

Convention: On this slide  $c'$  is not a derivative but just another name ...

## Virtual Substitution into Polynomial

Virtually substitute  $(a + b\sqrt{c})/d$  into a polynomial  $p$ :

$$p_{\frac{a+b\sqrt{c}}{d}} \stackrel{\text{def}}{=} p\left(\frac{a+b\sqrt{c}}{d}\right) \quad \text{by algebraic evaluation of } +, \cdot$$

## $\sqrt{c}$ -algebra

Algebra of terms  $(a + b\sqrt{c})/d$  with polynomials  $a, b, c, d \in \mathbb{Q}[x_1, \dots, x_n]$ :  
 where  $c \geq 0, d, d' \neq 0$

$$\begin{aligned} ((a + b\sqrt{c})/d) + ((a' + b'\sqrt{c})/d') &= ((ad' + da') + (bd' + db')\sqrt{c})/(dd') \\ ((a + b\sqrt{c})/d) \cdot ((a' + b'\sqrt{c})/d') &= ((aa' + bb'c) + (ab' + ba')\sqrt{c})/(dd') \end{aligned}$$

Convention: On this slide  $c'$  is not a derivative but just another name ...

## Virtual Substitution into Comparisons

Virtually substitute  $(a + b\sqrt{c})/d$  into a comparison  $p \sim 0$ :

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv$$

## Virtual Substitution into Comparisons

Virtually substitute  $(a + b\sqrt{c})/d$  into a comparison  $p \sim 0$ :

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0)$$

## Virtual Substitution into Comparisons

Virtually substitute  $(a + b\sqrt{c})/d$  into a comparison  $p \sim 0$ :

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0)$$

## $\sqrt{c}$ -comparisons

$$d \neq 0 \wedge c \geq 0$$

$$(a + 0\sqrt{c})/d = 0 \equiv$$

$$(a + 0\sqrt{c})/d \leq 0 \equiv$$

$$(a + 0\sqrt{c})/d < 0 \equiv$$

$$(a + b\sqrt{c})/d = 0 \equiv$$

$$(a + b\sqrt{c})/d \leq 0 \equiv$$

$$(a + b\sqrt{c})/d < 0 \equiv$$

## Virtual Substitution into Comparisons

Virtually substitute  $(a + b\sqrt{c})/d$  into a comparison  $p \sim 0$ :

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0)$$

## $\sqrt{c}$ -comparisons

$$d \neq 0 \wedge c \geq 0$$

$$(a + 0\sqrt{c})/d = 0 \equiv a = 0$$

$$(a + 0\sqrt{c})/d \leq 0 \equiv ad \leq 0$$

$$(a + 0\sqrt{c})/d < 0 \equiv ad < 0$$

$$(a + b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2c = 0$$

$$(a + b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \wedge a^2 - b^2c \geq 0 \vee bd \leq 0 \wedge a^2 - b^2c \leq 0$$

$$(a + b\sqrt{c})/d < 0 \equiv ad < 0 \wedge a^2 - b^2c > 0$$

$$\vee bd \leq 0 \wedge (ad < 0 \vee a^2 - b^2c < 0)$$

## Virtual Substitution into Comparisons

Virtually substitute  $(a + b\sqrt{c})/d$  into a comparison  $p \sim 0$ :

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0) \quad \text{accordingly for } \wedge, \vee, \dots$$

## $\sqrt{c}$ -comparisons

$$d \neq 0 \wedge c \geq 0$$

$$(a + 0\sqrt{c})/d = 0 \equiv a = 0$$

$$(a + 0\sqrt{c})/d \leq 0 \equiv ad \leq 0$$

$$(a + 0\sqrt{c})/d < 0 \equiv ad < 0$$

$$(a + b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2c = 0$$

$$(a + b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \wedge a^2 - b^2c \geq 0 \vee bd \leq 0 \wedge a^2 - b^2c \leq 0$$

$$(a + b\sqrt{c})/d < 0 \equiv ad < 0 \wedge a^2 - b^2c > 0$$

$$\vee bd \leq 0 \wedge (ad < 0 \vee a^2 - b^2c < 0)$$



## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

## Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$ )

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$\left( \exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow \right.$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\left. \vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge \left( F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)} \right) \right)$$

## Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$ )

Extended logic

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

FOL<sub>ℝ</sub>

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$(\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge (F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)})$$

## Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$ )

Extended logic

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

FOL<sub>ℝ</sub>

$$\omega_x^r \in \llbracket F \rrbracket \text{ iff } \omega \in \llbracket F_{\bar{x}}^{(a+b\sqrt{c})/d} \rrbracket \text{ where } r = (\omega[a] + \omega[b] \sqrt{\omega[c]}) / (\omega[d]) \in \mathbb{R}$$

# Example: Quadratic Curiosity

$$a \neq 0 \rightarrow (\exists x (ax^2 + bx + c = 0 \wedge ax^2 + bx + c \leq 0) \leftrightarrow b^2 - 4ac \geq 0 \wedge \text{true})$$

$$\begin{aligned} & (ax^2 + bx + c)_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac}) / (2a)} \\ &= a((-b + \sqrt{b^2 - 4ac}) / (2a))^2 + b((-b + \sqrt{b^2 - 4ac}) / (2a)) + c \\ &= a((b^2 + b^2 - 4ac + (-b - b)\sqrt{b^2 - 4ac}) / (4a^2)) + (-b^2 + b\sqrt{b^2 - 4ac}) / (2a) + c \\ &= (ab^2 + ab^2 - 4a^2c + (-ab - ab)\sqrt{b^2 - 4ac}) / (4a^2) + (-b^2 + 2ac + b\sqrt{b^2 - 4ac}) / (2a) \\ &= ((ab^2 + ab^2 - 4a^2c)2a + (-b^2 + 2ac)4a^2 + ((-ab - ab)2a + b4a^2)\sqrt{b^2 - 4ac}) / (8a^3) \\ &= (\cancel{2a^2b^2} + \cancel{2a^2b^2} - \cancel{8a^3c} - \cancel{4a^2b^2} + \cancel{8a^3c} + (-\cancel{2a^2b} - \cancel{2a^2b} + \cancel{4a^2b})\sqrt{b^2 - 4ac}) / (8a^3) \\ &= (0 + 0\sqrt{b^2 - 4ac}) / (8a^3) = (0 + 0\sqrt{\cdot}) / 1 = 0 \end{aligned}$$

$$(ax^2 + bx + c = 0)_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac}) / (2a)} \equiv ((0 + 0\sqrt{\cdot}) / 1 = 0) \equiv (0 \cdot 1 = 0) \equiv \text{true}$$

$$(ax^2 + bx + c \leq 0)_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac}) / (2a)} \equiv (\underbrace{(0 + 0\sqrt{\cdot}) / 1}_0 \leq 0) \equiv (0 \cdot 1 \leq 0) \equiv \text{true}$$

# Example: Nonnegative Roots of Quadratic Polynomials

$$a \neq 0 \rightarrow (\exists x (ax^2 + bx + c = 0 \wedge x \geq 0))$$

$$\leftrightarrow b^2 - 4ac \geq 0 \wedge (2ba \leq 0 \wedge 4ac \geq 0 \vee -2a \leq 0 \wedge 4ac \leq 0$$

$$\vee 2ba \leq 0 \wedge 4ac \geq 0 \vee 2a \leq 0 \wedge 4ac \leq 0))$$

$$\begin{aligned} -(-b + \sqrt{b^2 - 4ac}) / (2a) &= ((-1 + 0\sqrt{b^2 - 4ac}) / 1) \cdot ((-b + \sqrt{b^2 - 4ac}) / (2a)) \\ &= (b - \sqrt{b^2 - 4ac}) / (2a) \end{aligned}$$

$$(-x \leq 0)_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac}) / (2a)} \equiv ((b - \sqrt{b^2 - 4ac}) / (2a) \leq 0)_{\bar{x}}^x$$

$$\equiv b2a \leq 0 \wedge \cancel{b^2} - (-1)^2(\cancel{b^2} - 4ac) \geq 0 \vee -1 \cdot 2a \leq 0 \wedge \cancel{b^2} - (-1)^2(\cancel{b^2} - 4ac) \leq 0$$

$$\equiv 2ba \leq 0 \wedge 4ac \geq 0 \vee -2a \leq 0 \wedge 4ac \leq 0$$

$$(-x \leq 0)_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac}) / (2a)} \equiv ((b + \sqrt{b^2 - 4ac}) / (2a) \leq 0)_{\bar{x}}^x$$

$$\equiv b2a \leq 0 \wedge \cancel{b^2} - 1^2(\cancel{b^2} - 4ac) \geq 0 \vee 1 \cdot 2a \leq 0 \wedge \cancel{b^2} - 1^2(\cancel{b^2} - 4ac) \leq 0$$

$$\equiv 2ba \leq 0 \wedge 4ac \geq 0 \vee 2a \leq 0 \wedge 4ac \leq 0$$



- 1 Learning Objectives
- 2 Framing the Miracle
- 3 Quantifier Elimination
  - Homomorphic Normalization for QE
  - Term Substitutions for Linear Equations
- 4 Square Root  $\sqrt{\cdot}$  Virtual Substitution for Quadratics
  - Square Root Algebra
  - Virtual Substitutions of Square Roots
  - Example
- 5 Summary

## Virtual Substitution of $(a + b\sqrt{c})/d$ into Comparisons

$$(p \sim 0)_{\bar{x}}^{(a+b\sqrt{c})/d} \equiv (p_{\bar{x}}^{(a+b\sqrt{c})/d} \sim 0) \quad \text{accordingly for } \wedge, \vee, \dots$$

### $\sqrt{c}$ -algebra

$$d \neq 0 \wedge c \geq 0$$

$$((a + b\sqrt{c})/d) + ((a' + b'\sqrt{c})/d') = ((ad' + da') + (bd' + db')\sqrt{c})/(dd')$$

$$((a + b\sqrt{c})/d) \cdot ((a' + b'\sqrt{c})/d') = ((aa' + bb'c) + (ab' + ba')\sqrt{c})/(dd')$$

### $\sqrt{c}$ -comparisons

$$d \neq 0 \wedge c \geq 0$$

$$(a + b\sqrt{c})/d = 0 \equiv ab \leq 0 \wedge a^2 - b^2c = 0$$

$$(a + b\sqrt{c})/d \leq 0 \equiv ad \leq 0 \wedge a^2 - b^2c \geq 0 \vee bd \leq 0 \wedge a^2 - b^2c \leq 0$$

$$(a + b\sqrt{c})/d < 0 \equiv ad < 0 \wedge a^2 - b^2c > 0$$

$$\vee bd \leq 0 \wedge (ad < 0 \vee a^2 - b^2c < 0)$$

## Theorem (Virtual Substitution: Quadratic Equation $x \notin a, b, c$ )

$$a \neq 0 \vee b \neq 0 \vee c \neq 0 \rightarrow$$

$$(\exists x (ax^2 + bx + c = 0 \wedge F) \leftrightarrow$$

$$a = 0 \wedge b \neq 0 \wedge F_{\bar{x}}^{-c/b}$$

$$\vee a \neq 0 \wedge b^2 - 4ac \geq 0 \wedge (F_{\bar{x}}^{(-b + \sqrt{b^2 - 4ac})/(2a)} \vee F_{\bar{x}}^{(-b - \sqrt{b^2 - 4ac})/(2a)})$$

## Lemma (Virtual Substitution Lemma for $\sqrt{\cdot}$ )

Extended logic

$$F_x^{(a+b\sqrt{c})/d} \equiv F_{\bar{x}}^{(a+b\sqrt{c})/d}$$

FOL $_{\mathbb{R}}$

$$\omega_x^r \in \llbracket F \rrbracket \text{ iff } \omega \in \llbracket F_{\bar{x}}^{(a+b\sqrt{c})/d} \rrbracket \text{ where } r = (\omega[a] + \omega[b] \sqrt{\omega[c]}) / (\omega[d]) \in \mathbb{R}$$





André Platzer.

*Logical Foundations of Cyber-Physical Systems.*

Springer, Cham, 2018.

doi:10.1007/978-3-319-63588-0.



Volker Weispfenning.

Quantifier elimination for real algebra — the quadratic case and beyond.

*Appl. Algebra Eng. Commun. Comput.*, 8(2):85–101, 1997.

doi:10.1007/s002000050055.



André Platzer.

*Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.*

Springer, Heidelberg, 2010.

doi:10.1007/978-3-642-14509-4.



Jacek Bochnak, Michel Coste, and Marie-Francoise Roy.

*Real Algebraic Geometry*, volume 36 of *Ergeb. Math. Grenzgeb.*

Springer, Berlin, 1998.

doi:10.1007/978-3-662-03718-8.



Saugata Basu, Richard Pollack, and Marie-Françoise Roy.

*Algorithms in Real Algebraic Geometry.*

Springer, Berlin, 2nd edition, 2006.

doi:10.1007/3-540-33099-2.



Alfred Tarski.

*A Decision Method for Elementary Algebra and Geometry.*

University of California Press, Berkeley, 2nd edition, 1951.

doi:10.1007/978-3-7091-9459-1\_3.



George E. Collins.

Quantifier elimination for real closed fields by cylindrical algebraic decomposition.

In H. Barkhage, editor, *Automata Theory and Formal Languages*, volume 33 of *LNCS*, pages 134–183, Berlin, 1975. Springer.

doi:10.1007/3-540-07407-4\_17.